RFID - 1984 im 21. Jahrhundert

Lothar Binding[1], Matthias Melcher[2]

[1]Mitglied des Deutschen Bundestages
[2]Universitätsrechenzentrum Heidelberg
Im Neuenheimer Feld 293
69120 Heidelberg
[1]lothar.binding@bundestag.de
[2]matthias.melcher@urz.uni-heidelberg.de

Abstract: Ziel des Vortrags war es, gemeinsam mit dem Auditorium herauszufinden, ob hinter der Überschrift „RFID – 1984 im 21. Jahrhundert“ ein Fragezeichen oder ein Ausrufezeichen stehen sollte. Es gibt die juristische Auffassung, dass die RFID-Technologie in der Regel nicht unter das BDSG fällt. Deshalb genügten entsprechende Hinweise der Hersteller bzw. Anwender von RFID Tags und eine entsprechende Selbstverpflichtungsklausel der Industrie, des Handels etc., und eine gesetzliche Reglung sei entbehrlich. Dem gegenüber steht das allgemeine **Transparenz**prinzip des BDSG, d. h. die Verhinderung einer Situation, "in der Bürger nicht mehr wissen, wer was wann und bei welcher Gelegenheit über sie weiß".

Die Anwendungsmöglichkeiten der RFID-Technologie sind sehr vielfältig, weitreichend und aufregend. Die Mächtigkeit der alten Technologie in neuer Anwendung wird dabei besonders durch folgende Begriffe charakterisiert: unauffällig, eindeutig und genau, alles durchdringend und allgegenwärtig – kurz: **pervasiv** und **ubiquitär**. In der Verknüpfung von Objektdaten mit Personendaten wird eine völlig neue Dimension der Überwachung möglich – Bewegungsprofile, Kaufverhalten, Leseverhalten etc.

Deshalb bin ich der Auffassung, dass eine gesetzliche Regelung unumgänglich ist. Diese Auffassung wurde vom Auditorium der Tagung einhellig geteilt.

1 Die Historie

Es mag vielleicht überraschen, dass das ungeheure Potenzial der RFID-Technologie überhaupt nicht auf eine tiefgreifende technische Neuerung zurückzuführen ist, sondern schon sehr alte Wurzeln hat. Spätestens die Entwicklung des Radars kann als direkter Vorläufer angesehen werden.

Ihre Geschichte lässt sich damit folgendermaßen skizzieren:

- 1846 Michael Faraday – Licht und Radiowellen werden als Teil elektromagnetischer Energie erkannt.
- 1864 James Maxwell – Entwicklung der Theorie elektromagnetischen Felder.
- 1887 Heinrich Hertz – Sendet und empfängt als erster Wellen.
- 1896 Marconi – Funkt über den Atlantik.
- 1906 Ernst Alexanderson – Kontinuierliches Erzeugen bzw. Senden von Funkwellen
- 1922 Erfindung des Radars
- 1943 Erste Anwendung eines RFID Transponders im Zweiten Weltkrieg in Flugzeugen zur Freund- und Feindkennung
- 1948 Henry Stockman „Communication by Means of Reflected Power", wird oft als Geburtsstunde der Idee von RFID aufgefasst, viele praktische bzw. technische Probleme waren noch nicht gelöst.
- 60er Jahre – Erste kommerzielle Anwendung eines 1-bit-Transponders zur elektronischen Warensicherung.
- 70er Jahre – Erste Planung von Mauterfassungssystemen, Es beginnt die RFID basierte Tierüberwachung
- 80er Jahre – Eine stetig wachsende Zahl von Unternehmen setzen RFID-Technik ein, das Anwendungsspektrum wird ausgeweitet, erste Systeme zur Personenkontrolle.
- 90er Jahre – RFID in vielen Lebensbereichen: Bargeldloses Bezahlen, Skipässe, Zugangskontrollen, Kundenkarten etc.

Das also schon alte technische Prinzip stand meist im Schatten von anderen Identifikationsverfahren, die technisch spektakulärer, aufwändiger, interessanter waren, wie beispielsweise Zugangs-Karten für Beschäftigte oder neue IT-Praktiken wie Cookies für die Kunden im Web, oder die einfach deutlicher sichtbar waren, wie die Barcodes auf Waren. Erst die Kombination der Eigenschaften und Anwendungsmöglichkeiten aller dieser Verfahren hat der RFID-Technologie zu einem Potenzial verholfen, das nun allmählich Beachtung findet.

- 2005 RFID Technik in allen Lebensbereichen, in unserer Kleidung und allen Objekten bzw. Produkten, die wir uns denken können, auch im Reisepass biometrische Merkmalen

Viele der oben genannten neuen wisseneschaftlichen Erkenntnisse und fast jede technische Neuerung haben schon in der Vergangenheit zu übtriebener Euphorie ebenso

wie zu überbordender Skepsis geführt. Dies gilt ebenso für die Einführung von RFID – in der öffentlichen Diskussion mischen sich große Hoffnungen mit großen Befürchtungen.

Nachfolgend soll dieses Spannungsfeld beleuchet werden und im Ergebnis einige politisch-gesellschaftliche bzw. rechtliche Bedingungen genannt werden, unter denen die Hoffnungen gerechtfertigt und die Befürchtungen begrenzt werden können.

2 Ein wenig zur Technik

Das Prinzip der Radio Frequency Identification

Die Funktionsweise der Radio Frequency Identification ist gekennzeichnet durch folgende wesentliche Komponenten und Eigenschaften:

Die beiden wichtigen Komponenten sind

1. der **Transponder** bzw. Tag, ein im Regelfall drahtloses Kommunikations-, Anzeige- oder Kontrollgerät, das empfangene Signale auswertet und automatisch darauf antwortet.
   Der Begriff Transponder setzt sich zusammen aus Transmitter und Responder. Transponder können passiv oder aktiv sein. Sie heißen Datenträger, Label oder Tag, sind also "Etiketten" am zu identifizierenden Objekt,

2. das **Lesegerät** bzw. Reader, ein im Regelfall mit einer Schnittstelle zu einem Datenverarbeitungssystem versehener Empfänger.

Die beiden wichtigen Eigenschaften sind

3. die Identifizierung erfolgt über Funk, also durch kontaktlose Kommunikation über elektromagnetische Wellen, wobei die Lesegeräte nicht mit den Objekten in Berührung kommen müssen.

4. RFID-Systeme gehören zu den Auto-ID-Systemen, zum Identifizierungsakt ist somit kein Zutun des Besitzers oder irgendeines anderen notwendig, im Zweifelsfall wird die Identifizierung nicht einmal bemerkt oder kann nicht bemerkt werden.

Der Aufbau eines RFID-Systems

Das Schema der Kommunikationsarchitektur wird in der folgenden Skizze deutlich:

Der Transponder bzw. das Tag ist der passivste Teil: Energie und Takt werden vom Lesegerät an den Transponder geliefert. Bestimmte Daten fließen zunächst zum Transponder hin, sozusagen als Frage, anschließend von ihm weg, als Antwort – daher der Name Trans*ponder* wie Responder. Für den Träger des durch den Transponder gekennzeichneten Objekts passiert unscheinbar im Hintergrund die Verwertung der

Daten in einer Applikation auf einem Datenverarbeitungssystem, das seinerseits natürlich wieder vernetzt sein kann.

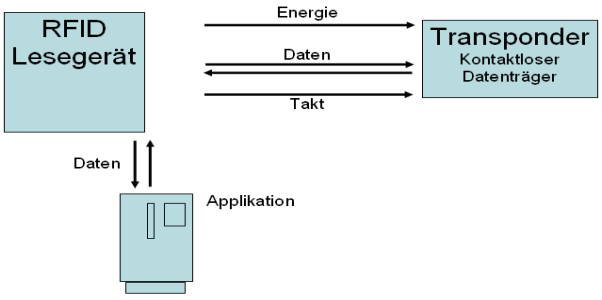


Abbildung 1: Schematischer Aufbau der RFID Kommunikationsarchitektur

Die Daten

Nun betrachten wir die Daten näher, die aus dem Tag abgerufen werden können. Ihre Strukturen sind in Normen bzw. Spezifikatifgonen festgelegt. Die wichtigste Norm dazu ist der Electronic Product Code, der EPC, vom Zentrum für Auto-ID am Massachusetts Institute of Technology, dem MIT, bei Boston.

EPC-Tag-Daten-Spezifikation

Solche Spezifikationen sind zwar oft sehr allgemein und auf eine ganze Klasse von Objekten anwendbar, aber diese ist doch außergewöhnlich: Die EPC-Spezifikation enthält ein Identifikationsschema zur *weltweit eindeutigen Kennzeichnung von physischen Objekten* – völlig allgemein: physische Objekte aller denkbarer Art! und dennoch: weltweit eindeutig!. Nicht nur der Waren*typ* wird identifiziert, sondern jedes einzelne Exemplar.

Die gemäß dem EPC definierten Daten unterliegen folgendem einheitlichen Gliederungsschema:

- Kopf: Kennzeichnung des nachfolgenden EPC-Nummernident, beispielsweise den SSCC-96, den Serial Shiping Container Code
- Filterwert (optional): Er zeigt an, um welchen Typ von Einheit es sich handelt, etwa Artikel, Palette oder Karton etc.
- Ein oder mehrere Wertefelder also insbesondere
    - die Partition, die festlegt, an welcher Stelle die EPC-Manager-Nummer und die Objektklassennummer getrennt werden müssen,
    - die EPC-Manager-Nummer als den Company Prefix, also die Kennzeichnung des Inverkehrbringers des Produkts,

- die Objektklassennummer mit der die Nummer des Produkts angegeben wird, ähnlich der Artikelnummer, und
- die Seriennummer als fortlaufende Nummer des Artikels.

Der EPC definiert eine Ziffernfolge mit einer Länge von mindestens 64 Bit gemäß EPC-64 oder 96 Bit nach EPC-96 oder auch, abhängig vom verwendeten Nummernident, einer Länge von bis zu 204 Bit.

Welche Daten enthält ein RFID –Tag?

Um sich die Daten besser vorstellen zu können, betrachten wir eine konkrete Ausprägung der EPC-Norm genauer: Typ 1 mit 96 Bits. (Siehe Abb. 2).

Wer sich hier an IP-Nummern oder MAC-Level-IDs erinnert fühlt, wird bemerken, wie ein paar Bit mehr Länge die Anzahl der möglichen Objekte gleich gewaltig vervielfältigt.

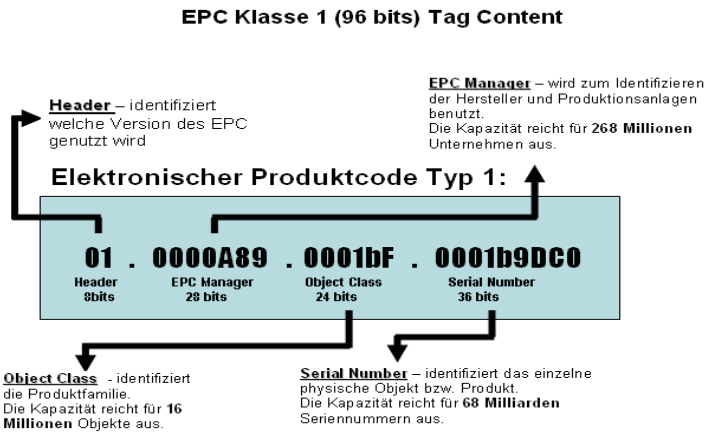


Abbildung 2: EPC Klasse 1 (96 bits) Tag Content

Diese kurze historische und technische Einordnung mag genügen um einen Eindruck zu haben, was RFID überhaupt ist und wie mächtig diese Technologie hinsichtlich der objektscharfen Kennzeichnung ist, wenn es in den folgenden Abschnitten um ihre Anwendungen und um die politischen und gesellschaftlichen Konsequenzen geht.

3 Die Anwendungen

Wir zeigen einen Vergeleich der RFID Technik , mit ähnlichen Techniken von Lange/Lammers anhand verschiedener wichtiger ökonomischer Parameter – unter Verzicht auf weitergehende Vergleiche, bezogen auf Parameter wie individuelle Selbstbestimmung, Zufriedenheit, Vertrautheit, Privatsphäre etc.

Stärken und Schwächen von Auto-ID-Techniken

Die folgende Grafik stellt die Stärken und Schwächen in Bezug auf fünf Kriterien im Vergleich zu dem bekannten Barcode[1] und dem 2D-Code[2] gegenüber: Sicherheit, Zusatzfunktionen, Effizienz, Leistung, und Kosten. Bei allen Parametern, mit Ausnahme der Kosten, liegt RFID klar vorne.

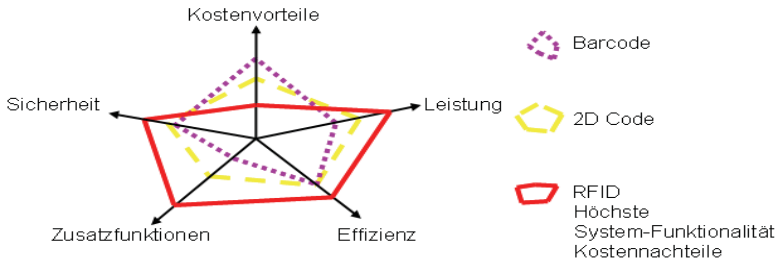


Abbildung 3: Stärken und Schwächen von Auto-ID-Techniken (Quelle: Lange/Lammers, Uni St. Gallen)

---

1 Ein linear oder eindimensionaler Code, kurz Barcode genannt. Er besteht aus einer Reihe von dünnen und breiten Linien, von verschiedenen Strichen und Lücken mit fester Breite, im Regelfall schwarz, auf einem oft weissen Hintergrund.

Als Beispiel hier der EAN 13 Code:

2 Ein 2d-Code besteht aus Gruppen von Quadraten oder Strichen auf einer quadratischen oder rechtwinkeligen Fläche. Aufgrund der zusätzlichen Dimension können 2d-Codes wesentlich mehr Information auf kleinstem Raum verschlüsseln als ein Barcode. Wir unterscheiden zwei verschiedene Varianten: den Stapelcode und den Matrixcode.

Als Beispiel hier der PDF 417 Code:

Was ist denn das Besondere an der RFID-Technologie? Irgendwie gab es das doch alles schon einmal in etwas anderer Form…

Besondere Kennzeichen: Pervasiv und Ubiquitär

RFID-Tags sind noch unauffälliger, noch genauer, noch eindeutiger und werden noch allgegenwärtiger und durchdringender sein als ihre Vorläufer. Die Schlagworte vom "ubiquitous computing" und von der "pervasive technology" treffen hier also in besonderem Maße zu. Grundlegende Techniken, wie Mikroprozessoren, Drahtlose Funktechnik und Datenübertragung durch universale Netze werden integriert.

RFID Einsatzpotentiale

Wie vielfältig die möglichen Einsatzbereiche sind und wie mächtig die Anwendung von RFID auf all unsere Lebensbereiche wirkt, zeigt folgende kleine Auswahl von Beispielen, die sich nach vielen verschiedenen Kriterien anordnen ließe und deshalb hier einfach alphabetisch geordnet ist:

- Abfallmanagement
- Bewegung von Alltagsgegenständen
- Bewegungsprofile von Inividuen
- Datenspuren
- Echtheitsprüfung von Dokumenten
- Energiemanagement
- Fahrscheine
- Fertigungsgeschichte
- Geräte-Sterilisation
- Instandhaltung, Reparatur
- Produkt-Authentifizierung
- Produktion und Warendistribution
- Prozesskontrolle
- Routenkontrolle
- Sicherheitssysteme
- Tieridentifikation
- Umweltmonitoring
- Verhaltens- und Denkprofile entlang der Lesegewohnheiten der Menschen
- Warenfluss-Management
- Wartung
- Wegfahrsperre
- Werkzeugkontrolle
- Zahlungssysteme
- Zutrittskontrolle

Integrierte Überwachung

In allen wichtigen Bereichen könnten die Vorgängersysteme möglicherweise durch RFID-Technologie abgelöst werden:

- Produkte Barcode, EAN etc.
- Kunden Cookies, Kundenkarten
- Mitarbeiter Keycards
- Bürger E-Pass[3]

Die Entwicklung läuft sicher auf mehr Integration hinaus. Integrierte Überwachung? Gesellschaftlich liegen die möglichen Entwicklungsrichtungen beliebig weit auseinander:

- Vertrauensvolle und dauerhafte Stammkunden-Beziehungen? Heile Welt?
- Immer mehr "Kleingedrucktes": Warnungen, Disclaimer, Einverständniserklärungen? Ohne Vertrauen, bürokratisches Erstickungspotential!
- Misstrauen, Argwohn und Wildwest-Methoden? Big Brother is watching You?

4 Der Einsatz

Schauen wir uns einige mögliche oder schon vorhandene und ökonomisch sehr erfolgreiche Einsatzszenarien an.

RFID im Handel

Die mögliche **Verbesserung der Logistikprozesse** ist eindrucksvoll:

- RFID beschleunigt den Transport vom Hersteller über den Handel zum Verbraucher
- Kontinuierliche Warenerfassung macht Inventuren überflüssig

---

[3] Mitte 2003 haben sich die Staats- und Regierungschefs der EU im Grundsatz darauf verständigt, biometrische Merkmale in die ePässe, also alle Reisedokumente, aufzunehmen.

Am 13. Dezember 2004 wurde folgerichtig eine Verordnung beschlossen die festlegt, dass innerhalb von 18 Monaten die Mitgliedsländer der EU Gesichtsbilder in digitaler Form in den Reisepass integrieren müssen.

Beispiel

- Die DHL bestückt Bekleidungsstücke mit Transpondern, um den Transport von China nach Europa sicherer und effizienter zu gestalten

RFID im Gesundheitswesen

Hier ist eine weitere **Erhöhung der Sicherheit** möglich:

- Fälschung von Medikamenten ist erkennbar
- Behandlungsfehler – Anamnese, Therapie, OP-Vorbereitung, Operationen werden evtl. vermieden, Identifizierung.

Beispiel

- Klinikum Saarbrücken: Ein Elektronisches Patientenarmband erlaubt den direkten Zugriff auf aktuelle Patientendaten.

RFID in der Industrie

Die mögliche **Verbesserung der Warenflusskontrolle** ist hier besonders eindrucksvoll:

- Die lückenlose und transparente Rückverfolgung von Produkten wird möglich
- RFID ermöglicht die technologische Umsetzung der EU-Richtlinie 178/2002 – Rückverfolgbarkeit von Lebensmitteln

Beispiel

- Der Spanische Rinderzuchtverband nutzt RFID-Transponder, um den Lebensweg hochwertiger Rinder zu dokumentieren.

RFID in der Logistik

Eine schon jetzt erkennbare besondere Stärke der RFID-Technologie ist die **Optimierung von Lieferketten**:

- Überwachung des Transportweges
- Gezieltere Nachbestellung von Waren
- Automatische Bestellkontrolle bei einem Wareneingang
- Kontrolle über Aufenthaltsort im Unternehmen
- Automatische Garantiebearbeitung
- Erleichterung von Rückrufaktionen

5 Und der Datenschutz?

Auf den ersten Blick könnten wir eigentlich sorglos in die Zukunft schauen…

- Das RFID-Chip selbst enthält „im Regelfall“ nur Zahlenfolgen zur Produktidentifikation oder Prozessinformation und ist scheinbar nicht in Verbindung zu sehen mit einem Individuum, einem Menschen…
- Auch in den verknüpften IT-Systemen werden nur produkt- oder prozessbezogene Daten gespeichert und verarbeitet…
- Speichern personenbezogener Daten, etwa durch Zugangskontrollen oder Kundenkarten ist gemäß BDSG nur mit persönlicher Einwilligung zulässig.

Und dennoch kann es gefährlich werden wenn jeder …

- sehen kann, wie viel Geld ich in der Tasche habe,
    - durch die Markierung von Euro-Banknoten
    - durch automatische Notierung von Seriennummern
- meinen Ausweis auslesen kann – trotz einer gewissen Zugangskontrolle durch „basic accesss control“ oder „extended access control“.
- meinen Einkauf Produktescharf auswerten kann
- über meine Aktentasche Bescheid weiß, über meine Bücher, also meine Leseinteressen, meine Medikamente, also meine Krankheiten…

Weiteren Gefahren ist nicht mit Sicherheit zu begegnen:

- Möglichkeit, dass nicht Berechtigte unbemerkt Informationen lesen
- Manipulation von Tags
- Unberechtigte Verknüpfung mit Personen

Es existiert also ein Privacy Problem:

- Erkennen von Personen
- Tracking von Personen
- Tracking von Produkten

Schon aus diesen wenigen aber tiefgreifenden kritischen Bemerkungen hinsichtlich Datensicherheit und Datenschutz leiten wir folgende Forderungen ab:

- Verbot ganzer Anwendungsfelder
    - Verfolgen von Personen
    - Anbringen von RFID-Tags an Münzen oder Geldscheinen
- Vollständige Transparenz bezüglich ausgelesener RFID-Daten,
- Keine Zentrale Speicherung

- Recht auf Zerstörung des RFID-Tags nach dem Kauf des „getagten“ Produktes
- Folgenabschätzung durch die Regierung
- Gesetzesinitiative durch den Gesetzgeber, Parlament, Regierung

Nachfolgend wird reflektiert, warum die gegenwärtigen Regelungen im Bundesdatenschutzgesetz nicht hinreichend sind.

Reichweite des §6c BDSG

Nach meinen Gesprächen mit den Experten des Bundesdatenschutzbeauftragten fällt die RFID nicht unter das Bundesdatenschutzgesetz (BDSG), weil ein RFID Tag lediglich am Produkt hänge. Im § 6c des BDSG werden die Bedingungen für „Mobile personenbezogene Speicher- und Verarbeitungsmedien“ definiert, so dass mit entsprechenden Hinweisen der Hersteller bzw. Anwender von RFID Tags und einer einsprechenden **Selbstverpflichtungsklausel** der Industrie, des Handels etc. eine gesetzliche Reglung entbehrlich sei. Bisher sei auch keine Rechtsprechung, kein Musterprozess zum Thema RFID und Datenschutz bekannt.

Auch wenn ein "Tag" nicht direkt an der Person "hängt", schreibt §6c BDSG besondere

Transparenzregeln für Chipkarten und andere "*mobile personenbezogene Speicher- und Verarbeitungsmedien*" vor, welche in § 3 Abs. 10 definiert sind, als "*Datenträger, die*

1. *an den Betroffenen ausgegeben werden,*
2. ***auf** denen **personenbezogene** Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert **verarbeitet** werden können und*
3. *bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.*"

Zu beachten ist die Einschränkung der Nummer 2 dieser Vorschrift, dass die automatisierte Verarbeitung **auf** dem Medium selbst stattfinden muss. Die direkte Kommunikation mit dem Lesegerät (Reader) reicht nicht aus. Die Unmerklichkeit der Datenübermittlung ist irrelevant.

Die Anwendbarkeit des Paragraphen 6c ist also strittig [Schütz 2006], obwohl seine *Absicht* klar auf die RFID anzuwenden ist: das allgemeine Transparenzprinzip des BDSG, d. h. die Verhinderung einer Situation, "in der Bürger nicht mehr wissen, wer was wann und bei welcher Gelegenheit über sie weiß".

Transparenz und Vertrauen

Das Transparenzgebot wird in den letzten Jahren auf eine harte Probe gestellt, insbesondere auch hinsichtlich der Spuren, die der Bürger und Kunde im Web hinterlässt. Immer wieder wird man durch Popup-Fenster genötigt, eine **Akzeptanz-Erklärung** anzuklicken, obwohl der zu akzeptierende Text unverschämt klein gedruckt und schlecht lesbar, lang und unverständlich ist. So wurde die Wirksamkeit der datenschutzrechtlichen Aufklärungspflichten immer weiter ausgehöhlt.

Die Folge beim Bürger ist eine Mischung aus Hilflosigkeit, Unbehagen und Unwissenheit gegenüber den Datenspeicherungspraktiken, die manchmal zu einer Art paranoidem Fatalismus führt, und schließlich auch zu wachsendem Misstrauen der Kunden gegenüber ihren Lieferanten.

Das verloren gehende Vertrauen sollte deshalb durch neue, wirksame Verfahren und Regelungen wiedergewonnen werden, die dem Bürger die unmittelbar sichtbare Sicherheit vermitteln, dass mit seinen Daten kein Missbrauch getrieben wird, am besten mit der öffentlichen Möglichkeit der **Einsichtnahme** in die Verarbeitungsprozesse.

Schon die bloße Möglichkeit dazu und evtl. das Wissen, dass ein Bekannter, von einem weiteren Bekannten oder Vertrauten… diese Möglichkeit irgendwann einmal tatsächlich wahrgenommen hat, hilft z. B. bei der Auszählung unserer geheimen Wahlen, dass das Vertrauen hier flächendeckend groß ist. Da das Misstrauen – oft gestützt auf eigene Erfahrungen – vieler Menschen in die Datenschutz-Praktiken der Wirtschaft riesig ist, wird deren Beseitigung eine große Aufgabe sein, die technisch eine neue Herausforderung und damit auch neue wirtschaftliche Impulse bietet. Wenn dann das Vertrauen wieder hergestellt ist, sollte die verbesserte Loyalität der Kunden abermals neue, langfristige wirtschaftliche Vorteile in Aussicht stellen.

Personenbezogen vs. personenbeziehbar

Befürchtungen, dass die Informationen die ein RFID Tag bereit hält und beispielsweise die im RFID Tag des Reisepasses enthaltenen Informationen, durch gleichzeitiges Auslesen durch RF Lesegeräte bekannt werden und kombiniert weiter verarbeitet werden könnten, teilt der Bundesdatenschutzbeauftragte nicht, weil insbesondere der Personalausweis durch den Freischaltcode „Basic Access Control“ bzw. künftig durch den „Extended Access Control“ geschützt sei.

Mit der Erkenntnis, dass es im Regelfall nur eine Frage der Zeit ist, bis solche Freischaltcodes „geknackt“ sind und mit dem Wissen, dass RFID Tags prinzipiell beliebige, auch personenbezogene Daten, verfügbar machen kann und in der Verknüpfung von Objektdaten mit Personendaten eine völlig neue Dimension der Überwachung möglich wird – Bewegungsprofile, Kaufverhalten, Leseverhalten etc. – bin ich der Auffassung, dass **eine gesetzliche Regelung unumgänglich** ist. Diese Auffassung wurde vom Auditorium der Tagung einhellig geteilt.

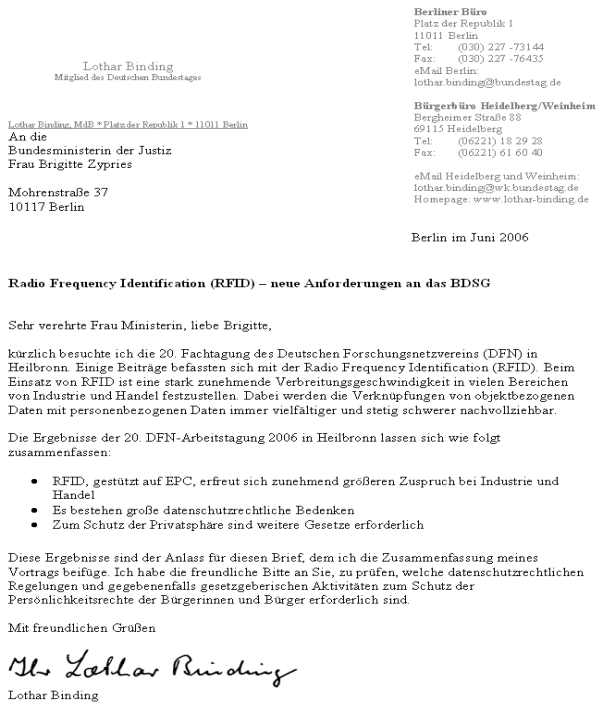
Die Regelung muss dem Transparenzgebot genüge tun. Angesichts des wachsenden Gefühls von Hilflosigkeit gegenüber den Datenschutz-Regeln in weiten Teilen der Wirtschaft, sollte dies nicht nur Aufklärungspflichten betreffen, die halbherzig durch immer mehr Kleingedrucktes erfüllt werden, sondern durch neue Wege und öffentliche Möglichkeiten der Einsichtnahme in die Prozesse, verbessert werden. Diejenigen Bereiche der Wirtschaft, die sich aktiv gegen einen möglichen Missbrauch engagieren, werden dabei sowohl technisch in Bezug auf Innovationswachstumsschübe profitieren wie auch längerfristig klimatisch durch größere Kundenloyalität.

6 Fazit und Ausblick

Die Ergebnisse der 20. DFN-Arbeitstagung 2006 in Heilbronn lassen sich wie folgt zusammen fassen:

- RFID, gestützt auf EPC, erfreut sich zunehmend größeren Zuspruch bei Industrie und Handel
- Es bestehen große datenschutzrechtliche Bedenken
- Zum Schutz der Privatsphäre sind weitere Gesetze erforderlich

Als praktische Konsequenz – Verknüpfung von Tagungsergebnis und praktischer Politik – schreibe ich entsprechende Briefe an den Bundesdatenschutzbeauftragten und das federführende Bundesministerium der Justiz.



Lothar Binding
Mitglied des Deutschen Bundestages

Berliner Büro
Platz der Republik 1
11011 Berlin
Tel: (030) 227 -73144
Fax: (030) 227 -76435
eMail Berlin:
lothar.binding@bundestag.de

Bürgerbüro Heidelberg/Weinheim
Bergheimer Straße 88
69115 Heidelberg
Tel: (06221) 18 29 28
Fax: (06221) 61 60 40

eMail Heidelberg und Weinheim:
lothar.binding@wk.bundestag.de
Homepage: www.lothar-binding.de

Lothar Binding, MdB * Platz der Republik 1 * 11011 Berlin
An die
Bundesministerin der Justiz
Frau Brigitte Zypries

Mohrenstraße 37
10117 Berlin

Berlin im Juni 2006

Radio Frequency Identification (RFID) – neue Anforderungen an das BDSG

Sehr verehrte Frau Ministerin, liebe Brigitte,

kürzlich besuchte ich die 20. Fachtagung des Deutschen Forschungsnetzvereins (DFN) in Heilbronn. Einige Beiträge befassten sich mit der Radio Frequency Identification (RFID). Beim Einsatz von RFID ist eine stark zunehmende Verbreitungsgeschwindigkeit in vielen Bereichen von Industrie und Handel festzustellen. Dabei werden die Verknüpfungen von objektbezogenen Daten mit personenbezogenen Daten immer vielfältiger und stetig schwerer nachvollziehbar.

Die Ergebnisse der 20. DFN-Arbeitstagung 2006 in Heilbronn lassen sich wie folgt zusammenfassen:

- RFID, gestützt auf EPC, erfreut sich zunehmend größeren Zuspruch bei Industrie und Handel
- Es bestehen große datenschutzrechtliche Bedenken
- Zum Schutz der Privatsphäre sind weitere Gesetze erforderlich

Diese Ergebnisse sind der Anlass für diesen Brief, dem ich die Zusammenfassung meines Vortrags beifüge. Ich habe die freundliche Bitte an Sie, zu prüfen, welche datenschutzrechtlichen Regelungen und gegebenenfalls gesetzgeberischen Aktivitäten zum Schutz der Persönlichkeitsrechte der Bürgerinnen und Bürger erforderlich sind.

Mit freundlichen Grüßen

Lothar Binding

Literaturverzeichnis

Lange, Dr. Volker, und **Lammers**, Dipl. Ing. Wolfgang (Institute of Technology Management, University of St. Gallen): Logistiktrends für Handel und Industrie, RFID 2004, 27.9.2004,

Schütz, RA Dr. Raimund (Freshfields Bruckhaus Deringer, Düsseldorf), RFID und datenschutzrechtliche Transparenz, in: Kommunikationsrecht - Die Monatsschau, zitiert nach MMR 2006, Heft 5, XX